AO 106 (Rev. 04/10) Application for a Search Warrant

AUSA Glenn-Applegate

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

2020 APR 15 PM 1:52

U.S. DIST. COURT
SOUTHERN DIST. OHIO
EAST DIV. COLUMBUS

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information and records associated with the cellular device assigned call number 614-316-6062 with electronic serial number 358503083164682 that is stored at premises controlled by T-Mobile

Case No. 2:20-mj-276

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of New Jersey , there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)	Receipt and Distribution of Child Pornography
18 U.S.C. § 875(d)	Interstate Communications with Intent to Extort
18 U.S.C. § 1028(a)(7)	Unlawful Transfer, Possession, or Use of a Means of Identification
See other offenses in affidavit	See other offense descriptions in affidavit

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

_____
Applicant's signature

Philip R. Jones, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: April 15, 2020

_____
Kimberly A. Johnson
United States Magistrate Judge

City and state: Columbus, Ohio

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE CELLULAR DEVICE ASSIGNED CALL NUMBER **614-316-6062**, WITH ELECTRONIC SERIAL NUMBER **358503083164682**, THAT IS STORED AT PREMISES CONTROLLED BY **T-MOBILE**	Case No. _____

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Philip R. Jones, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular telephone assigned call number **614-316-6062**, with Electronic Serial Number **358503083164682** ("the SUBJECT PHONE"), that is stored at premises controlled by T-Mobile USA, Inc, hereinafter "T-Mobile," a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, NJ 07054. The subscriber of this device is Osadebamwen Uwadiae; however, it is in the possession of and used by the subject of this investigation, Omoruyi Uwadiae, age 24, of Seattle, Washington. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require T-Mobile to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation and have been since January 2015. As part of my duties, I have investigated a wide variety of violations, to include crimes against children, extortion and crimes involving internet and cellular communications. I have gained

experience with the use of cellular telephones by individuals during the commission of crimes through these investigations, and I am aware that individuals involved in certain crimes often either utilize a cellular device during the commission of a crime, or they maintain such a device on their person at the time of the crime.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers, witnesses and an interview of Uwadiae. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252, 18 U.S.C. § 2252A, 18 U.S.C. § 875(d) and 18 U.S.C. § 1028(a)(7), the "Subject Offenses," have been committed by Omoruyi Uwadiae. There is also probable cause to search the information described in Attachment A for evidence and instrumentalities of these crimes as further described in Attachment B.

RELEVANT STATUTES

5. This investigation concerns alleged violations of 18 U.S.C. §§ 2252 and 2252A, 18 U.S.C. § 875(d) and 18 U.S.C. § 1028(a)(7).

6. 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2) prohibit a person from knowingly receiving or distributing any child pornography or any material that contains child pornography that has been mailed, or using means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

7. 18 U.S.C. § 2252(4)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any films, video tapes or other matter containing any visual depiction that has been shipped or transported using any means or facility of interstate or foreign commerce or which was produced using materials which have been mailed, shipped or transported, by any means including by computer, if (i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (ii) such visual depiction is of such conduct.

8. 18 U.S.C. § 875(d) specifies that whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, shall be fined under this title or imprisoned not more than two years, or both.

9. 18 U.S.C. § 1028(a)(7) prohibits a person from knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

PROBABLE CAUSE

Identification of Juvenile Victim

10. In July 2019, I became involved in an investigation ultimately leading to the identification of Uwadiae.

11. By way of background, Uwadiae moved to Seattle, Washington from Columbus, Ohio in approximately January 2019. His family maintained residency in Columbus, Ohio, and Uwadiae was employed by Procter and Gamble, headquartered in Cincinnati, Ohio. Uwadiae appears to have travelled to Ohio for a few days to a couple weeks at a time during 2019 to include, but not limited to, the months of March, May, August, September, October and November.

12. I learned that a 17-year-old male, hereinafter VICTIM,[1] communicated with Uwadiae via Snapchat on or about April 1, 2019.

13. For reference, Snapchat is a social media application accessible via mobile cellular devices that allow users to exchange messages, images and videos. The content of these messages disappears from users' devices approximately 24 hours after being viewed.

1 VICTIM's identity is known to law enforcement; however, it is withheld for the purpose of this affidavit as VICTIM was not yet 18 years old when criminal activity was first observed.

14. VICTIM had told Uwadiae that he was 18 when they first began communicating. Uwadiae requested that VICTIM send nude images via Snapchat, and VICTIM complied by sending sexually explicit files that VICTIM and another male had created earlier in 2019 while VICTIM was 17. VICTIM sent these files to Uwadiae while VICTIM was 17 years old.

15. After receiving these files from VICTIM, Uwadiae claimed that VICTIM blocked him on Snapchat, and Uwadiae demanded that VICTIM pay money in exchange for not sharing these images of VICTIM with VICTIM's family and friends.

16. VICTIM refused to pay, and Uwadiae began to distribute sexually explicit images of VICTIM via the internet to several individuals to include VICTIM's family members, friends, classmates and other internet users. Uwadiae told VICTIM and other recipients of these messages and images that he wanted to share the images with VICTIM's parents in order to see how they would react as Uwadiae did not believe VICTIM's parents would have a favorable reaction or opinion of VICTIM engaging in homosexual acts. Uwadiae also sought to embarrass VICTIM by sharing these files with VICTIM's friends believing they would not view VICTIM's sexual relationship with another male favorably.

17. On April 1, 2019, VICTIM's brother received nude images of VICTIM from Uwadiae. VICTIM's brother responded by telling Uwadiae the following on Snapchat:

a. April 1, 2019 at 13:55:56 UTC, VICTIM's brother to Uwadiae: Uhm update... I'm calling the cops and you will be charged with child pornography

b. April 1, 2019 at 13:56:20 UTC, Uwadiae to VICTIM's brother: He's 18

c. April 1, 2019 at 13:56:29 UTC, VICTIM's brother to Uwadiae: 17 dumb fuck

d. April 1, 2019 at 13:56:35 UTC, Uwadiae to VICTIM's brother: Lol sure

18. I obtained the above messages by serving a search warrant on Uwadiae's Snapchat account, display name "Pezopowe," issued in the United States District Court for the District of Colorado issued by the Honorable Magistrate Judge N. Reid Neureiter on October 24, 2019, reference case 19-SW-6058-NRN.

19. Uwadiae continued to distribute sexually explicit images of VICTIM that were created prior to VICTIM's 18th birthday on dates to include, but not limited to, April 26, 2019, July 14, 2019 and September 14, 2019.

20. On July 13, 2019, Uwadiae created a publicly viewable Facebook account, user identification number 100039195104667, using the maiden name of VICTIM's mother as the Facebook username. The publicly viewable display photograph depicted VICTIM holding a male's penis near VICTIM's mouth. The account's "about me" section contained the following statement, "Just want to talk about how you found out about [VICTIM's first name] and what you think about his lifestyle." Several of VICTIM's family members received private messages and friend requests from this account.

21. During this investigation, VICTIM's uncle was a frequent recipient of Uwadiae's messages as VICTIM's uncle often engaged in text message arguments with Uwadiae. On or about September 15, 2019, VICTIM's uncle appears to have given Uwadiae my work cellular telephone number, and I received a telephone call from Uwadiae on September 15, 2019. Uwadiae asked if I was an FBI agent and if I was investigating him. I denied knowledge of the investigation during this call.

22. After the call, I requested that VICTIM's uncle admonish Uwadiae that he was distributing child pornography if Uwadiae began communicating with VICTIM's uncle again. I was aware that Uwadiae had sent sexually explicit images of VICTIM to VICTIM's mother and other individuals on September 14, 2019.

23. Uwadiae began communicating with VICTIM's uncle via text message within a couple hours of calling me. Uwadiae was advised again via text message that he was distributing child pornography, and Uwadiae responded that he believed he could do what he wanted with VICTIM's images since VICTIM had sent the images to Uwadiae. Uwadiae demanded $500 from VICTIM's uncle in exchange for discontinuing the distribution of child pornography and to leave VICTIM and VICTIM's family alone.

24. Uwadiae began sharing sexually explicit images of VICTIM with VICTIM's uncle and VICTIM's other uncle via text message shortly after being admonished again that he was distributing child pornography.

25. For reference VICTIM's uncle exchanged the following messages with Uwadiae on September 15, 2019. These messages do not represent all content sent, and they are only intended to represent that Uwadiae was again advised that he was distributing sexually explicit images of a person before that person had turned 18 years old:

a. VICTIM's uncle to Uwadiae: Yes, but now you know he was a minor. Your [sic] committing a crime. Does that not matter to you?

b. Uwadiae to VICTIM's uncle: He told me he was 18, now suddenly he's not?

c. VICTIM's uncle to Uwadiae: He's 18 now but not when the pics and video were taken

d. Uwadiae to VICTIM's uncle: I posted them online but took it down since you guys said he was underage

e. VICTIM's uncle to Uwadiae: If you knew yesterday he was a minor, why were you still sending shit to me?

f. VICTIM's uncle to Uwadiae: Why would you want naked pics of [VICTIM's first name], a 17 year old boy?... You post them on facebook to destroy him.

26. Upon seizing Uwadiae's device on December 6, 2019, I noted that Uwadiae had retained approximately 82 images and 4 video files depicting VICTIM in sexually explicit acts prior to his 18th birthday. These files had been received on or about April 1, 2019, and many of the images appeared to be screen captures extracted from the video files. One of these images, a screenshot of a message sent to VICTIM's mother containing sexually explicit material of VICTIM, had a modification date of November 9, 2019, which generally indicates that the file was viewed or otherwise altered on that date.

Additional Adult Victims

27. During this investigation I became aware that Lieutenant (Lt.) Nick Konves, Columbus Police Department (CPD), Columbus, Ohio, was also investigating Uwadiae for similar extortion tactics involving adult victims in Ohio. These victims included TB, HW, KC and SP.[2] Additional information on contact with HW is contained later in this affidavit. I also became aware of Tacoma, Washington resident JG after JG contacted the FBI to file a complaint advising that he had also been victimized by a party now known to be Uwadiae.

28. I learned at a later time that Detective Doug Cunningham, Ohio State University Police Department (OSUPD), had launched an investigation into Uwadiae based on statements from students TG and PM. Additional information regarding contact with TG is available later in this affidavit.

Summary of Contact between Uwadiae and HW

29. On March 27, 2019, at approximately 3:00 PM, HW was using Grindr, and he began a conversation with a party now known to be Uwadiae.

30. For reference, Grindr identifies itself as a "gay social network and chat" application per its description on Apple iTunes' application store.

31. HW and Uwadiae exchanged face and nude photographs using Grindr, and HW provided his cellular telephone number to Uwadiae. At 5:54 PM, HW received a text message from a telephone number attributed to Uwadiae stating, "Pay me $200 and I won't post it pics, vids, number, and name online." HW offered to write a check, but Uwadiae demanded the money be transferred electronically and stated he would give HW an hour to decide. HW stated, "Go for it." Uwadiae replied, "I should post your shit? [HW's first and last name]." HW had not given Uwadiae his full name. Uwadiae told HW to pay him or he would get a bunch of random people texting him.

32. At 7:14 PM, HW received a text message from a second telephone number which stated, "Do you really want your nudes out there? For when you become a vet...."

2 Additional victims referenced in this affidavit are adult, but they are identified by their initials. Many of these individuals were not comfortable with their sexual preference being public knowledge.

33. On March 28, 2019 at 7:04 PM, HW received a text from a third telephone number which stated, "Ok I'll take $50 and leave you alone."

34. At 7:19 PM, HW received a text message from a fourth telephone number which stated, "$200 and I'll take it down [website link]." The text message included a screenshot of the website where HW's nude photographs had been uploaded. The upload included HW's full name, stated he lived in Columbus, and included HW's Instagram handle. The upload included two sexually explicit videos depicting HW.

35. During the course of this investigation, I served several administrative subpoenas on several telephone numbers utilized by Uwadiae and serviced by companies such as Pinger, TextNow and TextMe, which provided free text messaging services using wireless internet instead of traditional cellular telephone plans.

36. Uwadiae used telephone number telephone number 254-307-5054 to distribute child pornography to VICTIM's uncle on April 26, 2019. Pinger provided Internet Protocol (IP) Address connection logs during the time this particular telephone number was assigned to Uwadiae, and these IP connection logs indicated that Uwadiae connected to IP address 140.254.77.171 on March 27, 2019 at 10:03 PM. This IP address was serviced by Ohio State University, OCIO Enterprise Networking, 320 West 8th Avenue, Columbus, Ohio 43201, and it appears to be indicative that Uwadiae and the SUBJECT PHONE were physically located in the State of Ohio at the time he was sending threatening communications to HW.

Summary of Contact between Uwadiae and TG

37. TG, an Ohio State University student, chatted with the user of Grindr profile "visitor 25" beginning on or about September 1, 2019 while TG was in Columbus, Ohio. TG communicated with visitor 25, now known to be Uwadiae, until he realized that Uwadiae utilized photographs of different people to represent himself including photographs of white males and a black male. TG blocked Uwadiae on September 2, 2019.

38. On September 4, 2019, TG saw a Grindr message advising TG that he needed to contact Uwadiae. Uwadiae's location information on Grindr indicated that Uwadiae was 133 feet away from TG. Grindr uses a user's cellular device location to match other users by proximity.

39. TG received an Instagram message later that day stating that TG needed to have sex with the sender or pay $200.

40. Uwadiae began creating false social media accounts using pictures of TG stating, "this guy is gay, see pics for evidence." Uwadiae threatened to send messages received from TG to TG's family if TG did not message him. TG was fearful that his family would not accept him if they learned TG was possibly homosexual, and TG had sent Uwadiae messages to that effect during initial conversations with Uwadiae.

41. OSUPD served a search warrant for a Google Voice account utilized to communicate with TG. Google results indicated the user was Omoruyi Uwadiae.

42. OSUPD called Uwadiae on October 21, 2019. Uwadiae initially denied having Grindr, but he later admitted to his enjoyment catfishing people to see their reactions. Uwadiae confirmed opening two social media accounts under TG's name in order to disclose that TG was homosexual. Uwadiae confirmed asking for sex or $200 in exchange for not telling anyone about TG.

43. Per statements from both Uwadiae and TG, they met in person in Columbus, Ohio on September 3, 2019, and they undressed in front of each other, but they did not have sexual contact.

Additional Victims

44. During this investigation, Lt. Konves, Det. Cunningham and I have interviewed 33 victims of similar contact outlined above, and these victims resided in Washington, Ohio, Colorado, Illinois, Arizona, Kentucky and other states. For the sake of brevity, I am not including statements made by each and every party. I am currently in the process of attempting to speak with another 30 or more individuals who appear to have been victimized by Uwadiae since at least March 2019 based on electronic communications observed on Snapchat and by reviewing Uwadiae's devices seized pursuant to a federal search warrant.

Search Warrant and Interview of Uwadiae

45. On December 6, 2019, FBI Seattle facilitated a residential search warrant of Uwadiae's residence, 1627 15th Avenue, Apartment 1, Seattle, Washington, which was authorized by a search warrant issued in the United States District Court for the Western District of Washington by the Honorable Magistrate Judge Mary Alice Theiler, reference case MJ19-581.

46. Lt. Konves and I interviewed Uwadiae, and Uwadiae provided the following information after being advised of the voluntary nature of the interview and that Uwadiae was free to leave at any time:

47. Uwadiae explained that investigators would likely find mischievous text messages on his cellular telephone sent by Uwadiae in order to get a reaction. Uwadiae explained that these messages were often sexual in nature.

48. Uwadiae utilized the social media application Grindr for hookups with other males. Should the other party block Uwadiae, Uwadiae would want to know what had happened in order to get closure. Uwadiae often possessed nude images of the other party, and he would tell the other person that he had their images. Uwadiae asked for money in order to get a reaction and to see how far it could go. Uwadiae believed asking for money may be a way to get the individual blocking or ignoring Uwadiae to speak with him again. Some people told Uwadiae that they would pay him.

49. Uwadiae used CashApp to receive payment, and he provided CashApp information to people with whom he was communicating.

50. Uwadiae recalled the name, [VICTIM]. VICTIM had initiated contact with Uwadiae on Grindr, and VICTIM had told Uwadiae that he was 18 years old. VICTIM told Uwadiae that his birthday was in April.

51. Uwadiae was told by interviewers that VICTIM was not yet 18 years old when he sent nude photographs and that family members had told Uwadiae that he was not yet 18 years old. Uwadiae thought that people were lying to him when they said VICTIM was not 18.

52. Uwadiae explained that he was just involved in mischief without malicious intent. Uwadiae's actions were not fair to VICTIM, and Uwadiae apologized for what he had said to VICTIM.

53. Uwadiae explained that Grindr users wasted Uwadiae's time, which was precious to Uwadiae. Those leading Uwadiae on had wasted his time. Uwadiae explained that he did not need their money.

54. Uwadiae believed that he had these types of conversations with approximately a couple dozen people. Uwadiae later stated that he would not be surprised if the investigation yielded 50 victims. He may have been surprised to learn about 100, but he would have been surprised to learn about 200 victims.

55. Uwadiae explained that he was on his cellular telephone a lot, and he would have a lot of time.

56. Uwadiae had communicated with people in Columbus, Ohio, Seattle, Washington and other locations. Uwadiae attempted to communicate with local Grindr users based on his location at the time. Individuals, such as VICTIM, also initiated contact with Uwadiae on Grindr.

57. Uwadiae recalled KC, and that he had spoken with and hooked up with KC approximately one year ago. For reference, KC reported Uwadiae's activities to CPD. Uwadiae wanted KC to talk to him. KC had used a racial slur which caused Uwadiae to become riled up. Uwadiae told KC that he should not say racial slurs because Uwadiae had KC's photographs. Uwadiae posted that KC was racist on multiple, fictitious Grindr accounts. Uwadiae used fake email accounts, to include voyeur@mail.com and other email accounts, to create these fake accounts. He logged into and out of Grindr profiles in order to access multiple Grindr accounts at different times.

58. Uwadiae posted nude photographs of other individuals on malegeneral.com. Uwadiae explained that malegeneral.com users posted nude photographs on this website all the time, and he just wanted to join in.

59. Uwadiae was not sure how many times he had posted nude images of other individuals. Uwadiae estimated that he had posted photographs of approximately 20 people on malegeneral.com. Uwadiae believed that he had posted KC's photographs on this website.

60. Uwadiae recalled speaking with SP on Grindr, but Uwadiae was not sure where he was physically located while speaking with SP. For reference, SP reported Uwadiae's activities to CPD. Uwadiae believed that an Instagram account calling SP racist sounded familiar. Uwadiae observed that SP would only reply to white people. Uwadiae created a fake Grindr profile depicting himself as a white male, and SP responded to such an account. SP did not reply to an account Uwadiae utilized depicting himself as a black male. SP did not use any racial slurs with Uwadiae; rather, he did not reply when contacted by an account depicting the user to be a black male.

61. Uwadiae may have sent nude photographs of SP to SP's family, but he did not remember. This kind of action sounded like something he may have done.

62. Uwadiae had created fake Instagram accounts for other individuals, but he could not recall specific details or for whom he had created these accounts. Uwadiae may have created a fake Facebook account for VICTIM.

63. The name HW sounded familiar, and Uwadiae believed HW lived in Columbus, Ohio. For reference, HW had reported Uwadiae's activities to CPD. Uwadiae recalled just talking to HW, and Uwadiae may have demanded money from HW. Uwadiae thinks he put HW's nude photographs on malegeneral.com. HW always sent nude photographs to people, and HW sent two nude videos to Uwadiae via WhatsApp. Uwadiae acknowledged that he had cat fished HW.

64. Uwadiae utilized WhatsApp to communicate with others using a different telephone number he had obtained through Google Voice.

65. Uwadiae recalled chatting with JG about a month or so ago. For reference, JG reported Uwadiae's activities to the FBI. Uwadiae probably asked JG for the same things. Uwadiae did not need money, and he just wanted to get a reaction.

66. Uwadiae explained that he did not think what he was doing was bad, and he was just causing mischief. Uwadiae now knew that such actions were bad because VICTIM was not 18. He did not realize how his actions affected other individuals.

67. Uwadiae agreed that it may be a sign that his actions were not right when people told him they were reporting him to law enforcement.

68. Uwadiae was not sure how many images of VICTIM he had received or how many individuals may have received these images from him. Uwadiae recalled that a Facebook profile picture depicted VICTIM, and he replied, "Oh, yeah," when I explained that the picture also depicted a penis.

69. Uwadiae thought people were just trying to get him off VICTIM's back when they told Uwadiae that VICTIM was a minor. Uwadiae recalled VICTIM's uncle, but he did not recall specifics about their conversation.

70. Uwadiae believed that if he were to send images to individuals, he would lose control of how they were used by the receiving individual.

71. Uwadiae did not believe individuals had done anything bad enough to have their images distributed by Uwadiae in such a fashion. Uwadiae just wanted attention. Uwadiae assumed that such distribution of potentially embarrassing photographs might harm that person's reputation.

72. Uwadiae's actions were mostly telephone based, but he may have maintained images of VICTIM on a computer. Uwadiae wanted to delete VICTIM's photos right away, and he did not want any of the content anymore.

73. Uwadiae utilized a Virtual Private Network (VPN) so his IP addresses would be disguised, but he did not use VPN all the time. Uwadiae did not believe he was doing anything so bad, but he also did not want law enforcement contact. Uwadiae remarked that he guessed his actions were more than just mischief.

74. Uwadiae knew it was wrong to demand money from people in exchange for not sharing their photographs. Uwadiae defined this act as extortion. He did not want the money, but he did want to see how far he could push it.

75. Uwadiae explained that investigators reviewing Cash App would find transactions in which individuals sent Uwadiae money in exchange for not sharing their pictures. Uwadiae "made a lot" of money and estimated the figure to be approximately $1,000. Uwadiae explained that he did not want the money, but he thought it may be a way for him to get closure. Uwadiae thought it would be fair that people should get money back, and he offered to return double or triple the amount.

76. Uwadiae followed through on his statements that he would leave people alone and stop distributing their images if that person paid him.

77. Uwadiae demonstrated on his cellular telephone how he accessed Cash App. Uwadiae accessed a separate, locked profile containing several applications to include Cash App and social media applications.

Attribution

78. In addition to Uwadiae's admission outlined above, Uwadiae used several social media profiles and telephone numbers to communicate with victims. Several administrative subpoenas and court orders were served on multiple service providers during this investigation to include Facebook, Instagram, Snapchat, T-Mobile, Comcast, Pinger, TextNow, TextMe and Grindr. Location data, IP address subscriber information, and other account information maintained by cellular and internet service providers for these accounts resolved to Uwadiae or places visited by Uwadiae except for times in which Uwadiae appeared to be using a VPN.

Reason for Request

79. The purpose for this application is to obtain records necessary to demonstrate specific timeframes in which the SUBJECT PHONE was physically located in the Southern District of Ohio to determine venue for possible criminal charges. I am requesting records from February 26, 2019 through December 5, 2019.

80. Per Uwadiae's own statements, by demonstrating to me on December 6, 2019 and by reviewing records extracted from the SUBJECT PHONE, I have observed that Uwadiae maintained

evidence of criminal activity on the SUBJECT PHONE to include communications sent to and received by VICTIM, TG, and several other victims.

81. It should be noted that Uwadiae does not appear to have contacted victims by utilizing telephone number 614-316-6062. I am only aware of him calling me using telephone number 614-316-6062, and I received these calls on December 6, 2019, December 9, 2019 and April 6, 2019; however, I am aware the Uwadiae has utilized the physical cellular device serviced by T-Mobile to commit the crimes outlined above. Uwadiae simply installed and utilized additional applications on the SUBJECT PHONE such as Pinger, TextMe, TextNow, Facebook, Instagram, Grindr, Snapchat and others, which were accessible from the SUBJECT PHONE during the commission of the crimes previously described. Therefore, while the records requested would generally be related to non-criminal activities, the SUBJECT PHONE's connections to cellular networks used to transmit these calls, messages and internet connections would provide useful information about the SUBJECT PHONE's physical location during the times Uwadiae was engaged in criminal activity involving use of the SUBJECT PHONE.

82. For example, while Uwadiae was communicating with HW on March 27, 2019, he was also communicating with other unrelated parties via text message. The times of the text messages were interspersed with the times Uwadiae sent threatening communications to HW. Records and information sought from T-Mobile could provide additional information about the SUBJECT PHONE's location while Uwadiae was engaging in criminal conduct.

Request for Timeframe

83. I am aware through interviews of victims that Uwadiae began messaging Seattle, Washington residents on Grindr in January 2019. The earliest extortion related messages and use of false social media platforms to publicly embarrass victims attributable to Uwadiae appears to have begun on or prior to March 20, 2019. I interviewed TB, a Seattle, Washington resident, and he became aware of an Instagram page falsely pretending to represent TB and containing potentially embarrassing images on March 21, 2019. TB provided text message communications between he and a friend that indicated that

the Instagram page had been deactivated on or about March 20, 2019, but the Instagram account's activation date was unknown.

84. By reviewing Uwadiae's device, it appears that Uwadiae first travelled to Ohio after moving to Seattle, Washington on or about February 26, 2019. On February 18, 2019, Uwadiae sent a message, "Hey I'll be in Cincy next Tuesday – Thursday. Let's get dinner." On Tuesday, February 26, 2019, Uwadiae sent his roommate a text message apologizing for knocking over a glass of water. Uwadiae's roommate replied that he would try to dry it up, and he told Uwadiae to "Enjoy cinci."

85. On April 2, 2020, I received a request from Uwadiae via his attorney for content from Uwadiae's Google Drive, which I had assumed control on December 6, 2019. On April 3, 2020, I replied that Uwadiae would need to be more specific about the contents requested due to the content present on the drive and the nature of Uwadiae's activities. Uwadiae specified via his attorney that he would like access to photographs taken prior to January 2019 except for photographs related to certain trips to include a trip to Columbus, Ohio in September 2019. Uwadiae's request for content prior to January 2019 appears to be indicative that Uwadiae recognized he began potentially illegal activities in January 2019.

Use of Other Investigative Tools

86. I recognize that records for IP address connections can often yield the location of a device connecting to the internet, such as the SUBJECT PHONE; however, Uwadiae periodically used a VPN connection to mask his true IP address. Some records I have reviewed would tend to indicate the device was connecting in France, when in reality it was likely located in the United States, while other IP address information indicated that the device was connected to a wireless network without a specific physical location being identifiable. In yet other instances, IP address records yielded specific, and likely accurate, locations of usage such as Uwadiae's residence in Seattle, Washington or at his family's residence in Columbus, Ohio; however, a review of IP addresses alone does not appear to present of clear picture of specific periods of time in which Uwadiae was physically present in Ohio.

87. I have in my possession flight records from several different airline carriers; however, such records only provide location information for a certain point in time at the beginning and end of

travel. Uwadiae generally flew into Ohio by using both John Glenn Columbus International Airport in Columbus, Ohio and Cincinnati/Northern Kentucky International Airport (CVG), physically located in Hebron, Kentucky. Uwadiae was noted to fly using multiple carriers to include Delta, United, Southwest and Air Alaska. Uwadiae may have used additional carriers currently unknown to travel to Ohio.

88. I have located numerous messages sent by Uwadiae during a review of his cellular telephone in which Uwadiae indicated that he was in Ohio on certain dates or in which Uwadiae stated he was planning to be in Ohio on a certain date, but these statements do not necessarily provide full reference for the duration of Uwadiae's several trips to Ohio. Similarly, I have reviewed statements made by Uwadiae and others indicating certain dates Uwadiae was physically located in Ohio, but like the other methods of location data previously described, they did not provide context for when Uwadiae arrived in Ohio or when he departed.

89. I have located a limited number of device location coordinates in an extraction of Uwadiae's cellular device, but these points are limited to November 2019, and they did not provide context for when Uwadiae arrived in Ohio or when he departed. Service providers such as Facebook have also provided device location data for connection times, but these results have generally only yielded a single date and time of location per records return.

90. From February 26, 2019 through December 5, 2019, Uwadiae sent and received approximately 14,507 text messages, as well as approximately 1,700 voice calls and 1,048 Multimedia Messaging Service (MMS) messages. The records being sought for these connections would be useful to further identify the physical location of the SUBJECT PHONE at the time these connections were made.

91. I currently have no reason to believe that anyone other than Uwadiae maintained possession and use of the SUBJECT PHONE.

OVERVIEW OF RELEVANT TECHNOLOGY

92. In my training and experience, I have learned that T-Mobile is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service

have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.

93. Based on my training and experience, I know that T-Mobile can collect cell-site data about the SUBJECT PHONE. I also know that wireless providers such as T-Mobile typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

94. T-Mobile stores such data for a period of two years, and therefore preservation of records being sought is generally not required.

95. Based on my training and experience, I know that T-Mobile also collects per-call measurement data, which T-Mobile also refers to as the "TrueCall," which is T-Mobile's version of Range To Tower (RTT) measurements. RTT data estimates the approximate distance of the cellular device from a cellular tower based on the speed with which signals travel between the device and the tower. This information can be used to estimate an approximate location range that is more precise than typical cell-site data.

96. Based on my training and experience, I know that wireless providers such as T-Mobile typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for

wireless telephone service. I also know that wireless providers such as T-Mobile typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the SUBJECT PHONE's user or users and may assist in the identification of the SUBJECT PHONE's location at the time of these crimes.

AUTHORIZATION REQUEST

97. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

98. I further request that the Court direct T-Mobile to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on T-Mobile, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Philip R. Jones
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on April 15, 2020, 2020

Kimberly A. Johnson
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number **614-316-6062**, Electronic Serial Number **358503083164682** ("the Account"), that are stored at premises controlled by T-Mobile ("the Provider"), headquartered at 4 Sylvan Way, Parsippany, NJ 07054.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period February 26, 2019 through December 5, 2019:

a. The following information about the customers or subscribers of the Account:

   i. Names (including subscriber names, user names, and screen names);

   ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

   iii. Local and long distance telephone connection records;

   iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

   v. Length of service (including start date) and types of service utilized;

   vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

   vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

   viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:

i. Records of user activity for each connection made to or from the Account, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses;

ii. Information about each communication sent or received by the Account, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers);

iii. All data about which "cell towers" (i.e., antenna towers covering specific geographic areas) and "sectors" (i.e., faces of the towers) received a radio signal from the cellular telephone or device assigned to the Account, to include all voice, SMS, MMS, and data activity; and

iv. All records containing round-trip-distance measurements and/or timing advance information for each connection made to or from the Accounts (GSM, CDMA, EVDO, UMTS, LTE, etc.), to include NELOS, RTT, True Call Measurement Data, PCMD records, and Reveal Reports.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence and instrumentalities of violations of 18 U.S.C. §§ 2252, 2252A, 875(d) and 1028(a)(7) involving Omoruyi Uwadiae during the period February 26, 2019 through December 5, 2019.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by T-Mobile, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of T-Mobile. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of T-Mobile, and they were made by T-Mobile as a regular practice; and

b. such records were generated by T-Mobile electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of T-Mobile in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by T-Mobile, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature